Public Safety Wireless Network

PSWN

Semiannual Commercial Digital Packet Data Services Assessment Update

June 1998

CELLULAR DIGITAL PACKET DATA

This document describes various aspects of cellular digital packet data (CDPD). It provides only a "snapshot" of CDPD services today, recognizing that technology is evolving, and industry is introducing new services and capabilities at a rapid pace. This document is not intended to reflect a government position or endorse a particular service provider or service. Rather, it is provided to offer broad industry information on CDPD. We invite comments to ensure that the most current information is included in our analyses.

If you have comments regarding the information contained in this document, please contact the Public Safety Wireless Network (PSWN) Program Management Office (PMO) at 800-565-PSWN or access the PSWN Program Home Page at: www.pswn.gov.

Public safety agencies rely heavily on their land mobile radio (LMR) networks for communications and coordination within and among organizations. In the past few years, commercial services such as cellular telephones and paging have provided powerful capabilities that complement existing public safety networks. It is important that public safety communities carefully evaluate, assess, and maintain current information on the expanding commercial wireless marketplace. This allows informed, objective assessments that will ultimately meet mission requirements.

The Increasing Importance of Wireless Data Services

Emerging wireless data services potentially provide greater efficiency for the mobile work force. Mobile data applications are an increasingly important communications tool for government, business, and private users. Data applications, such as electronic mail and database look-ups (e.g., name searches or license plate queries), are also becoming increasingly important for mobile users. Commercial carriers have developed a variety of wireless data services to meet this growing need. One of these services is cellular digital packet data (CDPD). This report describes CDPD services, discusses some of the key CDPD performance characteristics, provides sample costs, lists some considerations in selecting CDPD services, and provides a checklist to assist in determining whether CDPD meets user needs.

What is CDPD?

CDPD is a wireless data service that uses the cellular network to provide packet data capabilities. In fact, CDPD uses a data format similar to the one used for Internet communications. This allows most data applications to be supported through CDPD services. CDPD divides information into "packets" of data that are transmitted over the cellular network. Important CDPD considerations and definitions are illustrated in Exhibit 1.

Availability	Identifies whether CDPD services can be acquired from a carrier in a given region
Coverage	Identifies whether CDPD transmissions can reach users in a given service area
Reliability	Identifies whether users can access and use CDPD services during congestion or network disruption
Transmission Speed	Describes the end-to-end data speed, including call set-up time and transmission speed
Privacy and Security	Describes the level of inherent privacy and security of the service and the capability to add security measures
Cost	Characterizes the costs typical of CDPD services

Exhibit 1
Key CDPD Characteristics

Availability

At this writing, CDPD is available in more than half of the geographic United States and in 30 international markets. CDPD carriers use "roaming" agreements to extend their regional services to other areas outside their region. Therefore, as long as CDPD services are available, CDPD subscribers can use CDPD as they cross service areas or if they are on travel to different parts of the US.

Coverage

Carriers will typically deploy networks to provide services in areas with high population density, such as metropolitan areas and along roadways. Consequently, carriers may not provide full coverage in rural areas or beyond these major roadways. This is a key consideration for users that expect and need contiguous service off the beaten path.

Whether in the carrier's region or when roaming, CDPD users will often experience coverage gaps similar to cellular voice services. This often occurs in less populated areas or away from major roads. Coverage gaps can be caused by terrain or buildings that interfere with the signal. They are also due to "dead spots" within the region, where the carrier's signal is too weak or non-existent. Users should match operational requirements to CDPD coverage considerations to ensure the service is available when and where they need it.

Reliability

Users of commercial systems share the airwaves and compete for capacity with one another. Therefore, users may experience congestion if there is more demand than network capacity. Congestion within CDPD networks will cause delays in setting up a connection and transmitting information.

The likelihood and effect of congestion depends, in part, on the type of CDPD network implemented. The two network types are channel hopping networks and dedicated channel networks.

CDPD channel hopping takes advantage of capacity unused by cellular voice subscribers to transmit information. This means that the capacity available for CDPD is directly associated with the level of use by cellular voice calls. During peak periods or emergencies when voice traffic on cellular networks tends to increase significantly, the likelihood of CDPD users experiencing congestion may increase significantly – causing call set-up and transmission delays.

The other configuration uses dedicated channel networks. This technique dedicates capacity on a portion of the cellular network that is available for CDPD use only. Therefore, CDPD capacity does not vary as cellular voice calls increase or decrease. CDPD transmissions do not compete with cellular voice calls. To the CDPD user, this is an important improvement because CDPD performance is not affected when the cellular voice system is congested. Users must still compete with other CDPD users for call setup and channel capacity.

Cellular carriers will often use channel hopping when they first introduce CDPD service, in smaller cities, or where CDPD usage is low. They will implement dedicated channels in larger cities where the service has been offered for a number of years and demand is high. These network implementation strategies have significant implications for reliability. Users should exercise caution to ensure that service reliability will not affect critical operational requirements.

Transmission Speed

CDPD can provide a maximum link data rate of 19.2 kilobits per second (kbps). The actual user transmission speeds are less – typically from 10 to 12 kbps – when the application overhead is included [1]. The exact transmission speed varies among vendors and is affected by the level of traffic on the network. This can mean a 10 kilobyte file (which contains approximately 1500 words, or 3 text pages) will take up to 15 seconds to transmit. Times to send files of different sizes are provided in Exhibit 2 [2].

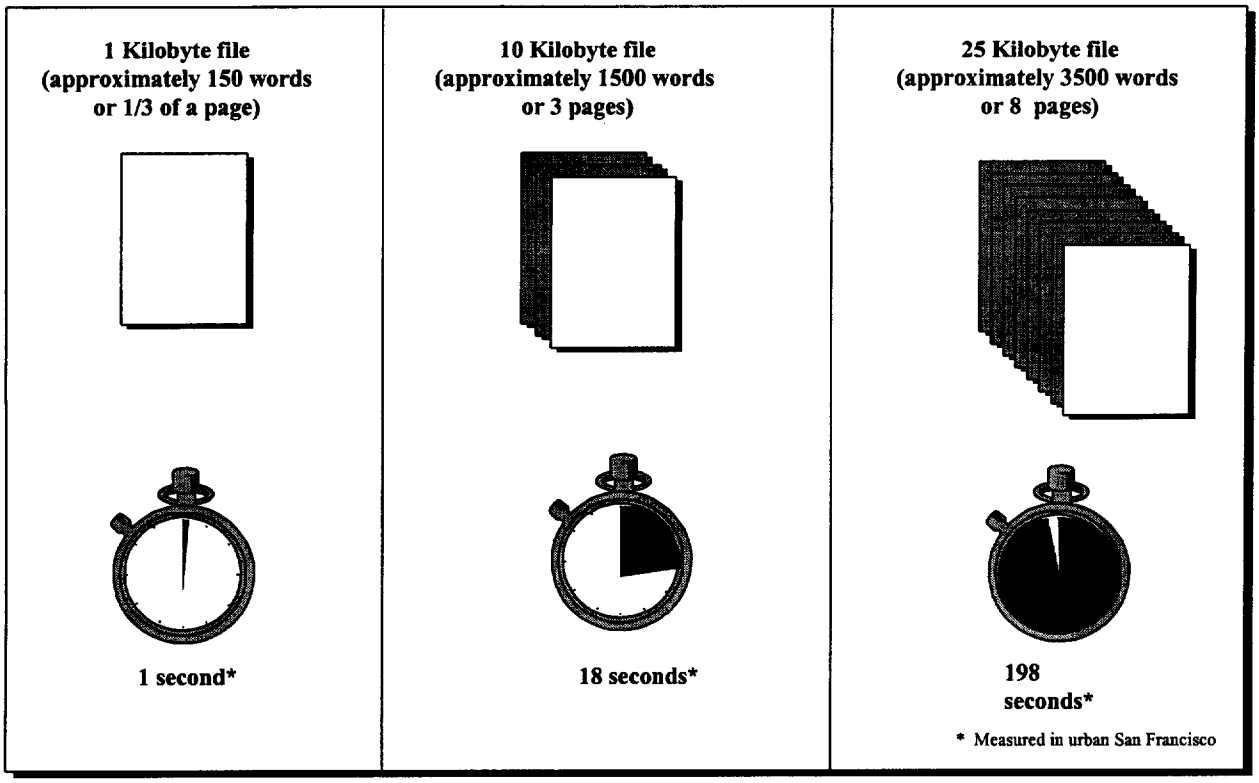

Exhibit 2

Sample Transmission Times for Different Sized Files

Call Set-Up Times

Call set-up time is the time it takes to begin transmitting information after the user pushes the transmit button. CDPD call set-up times range from less than 1 second to 3 or 4 seconds [3]. Differences in call set-up times may depend on the user terminal processing speed and the users' ability to access the network.

From the user's point of view, the overall time to transmit data is equal to the call set-up time plus the transmission duration. Using the example from above, the overall time needed to transmit a 10 kilobyte file is 18 seconds (3 seconds for set up and 15 seconds for transmission).

Privacy and Security

CDPD privacy features include automatic identification and authentication, to limit unauthorized, fraudulent access and data interception. Channel-hopping transmissions are more difficult to intercept than dedicated channel transmissions, since they often change channels between transmission of packets. However, intercepting channel-hopped communications is possible. CDPD does use a standard form of encryption to protect information sent over the air. For users with

more robust security requirements, end-to-end encryption schemes should be considered. Users should also consider the security practices of the service provider, with the respect to physical, operational, and information security.

User Equipment

Users typically require two pieces of equipment to use CDPD services: a CDPD modem and a user terminal. Key factors to consider when purchasing CDPD modems and user terminals for mobile users include functionality, device ruggedness, ease of use, battery life, computational power, display quality, warranty, and cost.

CDPD Modem

The CDPD modem includes the wireless antenna and the modem that provides compatibility with the CDPD network. CDPD modems can either be internal to the user terminal (built-in or removable, such as a PCMIA card) or external through a standard port. Because CDPD modems are based on personal computer standards, they are not specific to a particular carrier or manufacturer. CDPD modems typically range from $450 to $1000, depending on functionality and performance [4]. Users can buy standard CDPD modems from a number of manufacturers and use them on any CDPD network.

User Terminal

Any device that supports IP-based data communication can use CDPD. Business users employ different types of user terminals, which vary in terms of size and utility: notebook or laptop Personal Computers (PCs), handheld computers or PCs, pen-based computers, Personal Digital Assistants (PDAs), and wireless handsets. User terminal costs vary significantly based on the level of functionality, processing power, display characteristics, and vendor

CDPD from a Network-Level Perspective

CDPD is a packet data service that uses the existing analog cellular network infrastructure. Exhibit 3 describes the transmission of user information from a mobile user device to a database that is located in the user's office. When the user hits the transmit button, the information is divided into packets and bundled with "overhead" information about the route and destination address of the distant computer or terminal. For the example in Exhibit 3, this end-point is shown as the user database. These packets are sent over the airwaves and received by a nearby cellular antenna, where it enters the CDPD network.

From this point, the packets are routed to the local CDPD switch. Based on the routing information, the switch directs the data to the user's local network and, eventually, to the target database. As in Exhibit 3, the information retrieved from the database would generally be routed back along the same path to the CDPD user.

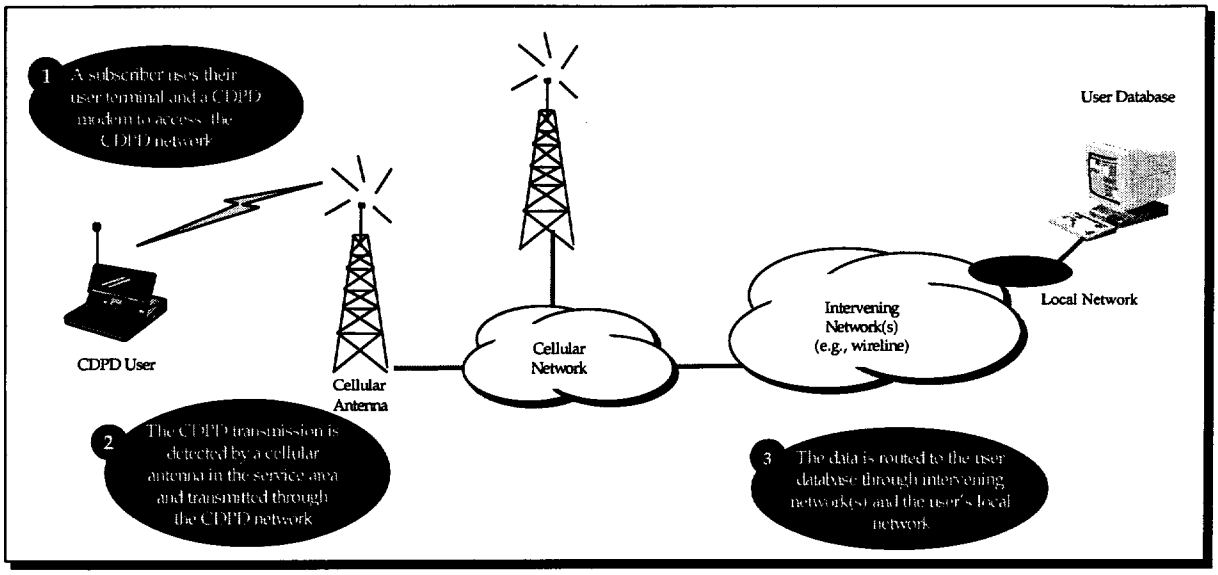

Exhibit 3
CDPD from a Network Perspective

CDPD Costs

Service pricing structure and service rates vary by carrier and pricing plan. There are currently two major types of pricing plans: flat rate and usage based.

For flat-rate pricing, users pay a set amount for unlimited usage. This pricing plan is advantageous to those who expect to make heavy use of CDPD services.

The second pricing plan uses a two-tiered approach. Users pay a set monthly price that allows for a fixed level of usage, and then they pay incrementally, on a per-kilobyte-transmitted basis, for usage beyond the fixed limit. Usage costs may vary depending on whether the user is calling within the carrier region or the user is roaming in another carrier's region. A typical pricing plan is shown in Exhibit 4 [5].

SERVICE PLAN	PLAN TYPE			
	A	B	C	D
Monthly Access Charge	$14.95 (150 Kb Allowance)	$29.95 (400 Kb Allowance)	$49.95 (1,100 Kb Allowance)	$89.95 (4,000 Kb Allowance)
Additional Per Kb Charge Over Plan Limit (In Region)	$0.10	$0.08	$0.05	$0.04
Additional Per Kb Charge Over Plan Limit (Out of Region)	$0.10	$0.10	$0.10	$0.10

Exhibit 4
Example Pricing Plan

CDPD Considerations

Users must think carefully about what commercial services may meet their operational requirements. Exhibit 5 provides some considerations in selecting CDPD services. Remember that CDPD service packages and billing structures are likely to vary among carriers. Before acquiring CDPD services, potential users may choose to employ the checklist at Exhibit 6 to assist in determining whether CDPD meets their needs.

CDPD Considerations

- **Cost**— CDPD prices are based on the amount of data rather than the length of time over which communications occur. Therefore, a user can maintain access to the network and incur charges only for the data exchanged. This is important if a connection must be maintained for an extended period.
- **Mobility**— CDPD may be used while traveling at high speeds. It has been tested traveling at speeds more than 85 miles per hour resulting in no signal degradation.
- **Transmission Speed**— CDPD can provide wireless data communications at speeds up to 19.2 kbps. The actual transmission speed is 10 to 12 kbps. This is considered good relative to other wireless data services.
- **Compatibility**— CDPD supports multiple protocols, which allows access to many networks and databases.
- **Flexibility** - With CDPD, there is no need to build a private network, reducing initial costs. Users can quickly adopt new services, and scale up to meet expanding needs. Users may also switch between service providers in areas with more than one provider offering CDPD services.
- **Coverage**— Although CDPD is available in most major metropolitan areas, rural coverage is sparse. Cellular carriers are continuing to implement CDPD in their cellular networks to expand CDPD coverage.
- **Roaming**— Although inter-carrier agreements have been signed among several carriers, additional agreements must be created to provide uninterrupted nationwide coverage.
- **Coverage Gaps**— Some CDPD networks may have gaps in coverage, depending on geographic terrain, shadowing from buildings, and network build-out.
- **Reliability**— It is likely that data transmission may be delayed if the cellular network becomes congested. Delays are more likely to occur on channel hopping than on dedicated channel CDPD implementations.

Exhibit 5
Considerations in Adopting CDPD Services

CDPD CHECKLIST

- ☑ Do I need a mobile data service?
- ☑ Where do I need mobile data services? Locally? Regionally? Nationally?
- ☑ What data services are available to meet my needs? Will this work in my current operational environment?
- ☑ Will it support mission-critical requirements?
- ☑ What is the coverage of the carrier's CDPD network?
- ☑ Do known coverage gaps exist? Where?
- ☑ Will the provider address my coverage gaps in areas where I know I will need CDPD services?
- ☑ Are there regional or nationwide roaming agreements? With whom?
- ☑ Is the provider's network a dedicated or a channel hopping network?
- ☑ What is the average transmission speed?
- ☑ What maximum delay in accessing the network will the carrier guarantee?
- ☑ What type of service and pricing plans are offered?
- ☑ How do the service plans rate against my needs?
- ☑ Are volume discounts or flat-rate pricing plans available?

Exhibit 6

User Checklist of Questions to Better Understand the CDPD Service

APPENDIX A
LIST OF ACRONYMS

CDPD	Cellular Digital Packet Data
IP	Internet Protocol
Kb	Kilobyte
kbps	Kilobits per second
LMR	Land Mobile Radio
MDT	Mobile Data Terminal
PC	Personal Computer
PDA	Personal Digital Assistants
PMO	Program Management Office
PSWN	Public Safety Wireless Network

APPENDIX B
REFERENCES

1. 10-12 kbps transmission speeds.
   AT&T Wireless Service, "AT&T Wireless Services Data Developer White Paper: Wireless Data Network Comparison," (1997), pp. 1-25.

2. File Transmission Speed Graphic
   Telephone conversation with James Straight, Bell Atlantic, McLean, VA., April, 1998.

3. CDPD Call Setup Times
   Vahid, Koussari, "Wireless Networking With Cellular Digital Packet Data," (1995). Obtained from City College of New York Web site:
   http://www.sci.ccny.cuny.edu/~koussari/wireless/wireless.html

4. CDPD Modem Costs
   Tabibian, Ryan O, "Wireless Data Shootout," Mobile Computing & Communications Magazine (1997). Obtained from Web site:
   http://www.mobilecomputing.com/articles/1997/03/9703cr2a.htm

5. CDPD Pricing
   Bell Atlantic Mobile, "Pricing Plans." (1998). Obtained from *Bell Atlantic Mobile Web site:* http://www.bam.com/amy_data/pricplan.htm

APPENDIX C
BIBLIOGRAHPY

Amorosa, Michael. "Commercial Services and Public Safety." Radio Resource, Pandanta Corp. August 1997. pg. 35.

"AT&T Wireless Services Data Developer White Paper: Wireless Data Network Comparison." AT&T Wireless Services. 1997. pp. 1-25.

Bell Atlantic Mobile (1998). "Pricing Plans."
Bell Atlantic Mobile Web Site
http://www.bam.com/amy_data/pricplan.htm

Bouvet, Stephen. Wireless Business and Technology, "1998:Pivotal Year for CDPD." February, 1998. pp. 34-38.

Coates, Bob. "Wireless Field Automation Delivers Results." Radio Resource, Pandanta Corp. August 1997. pp. 50-52.

Emigh, Jacqueline. "Cops Catch Bank Robbers Via RF-Enabled PC Laptops." Wireless Integration, Penwell Publishing. January, 1998. Pg. 42.

Green, James harry. 1997. The Irwin Handbook of Telecommunications. Chicago, Illinois: Irwin Publishing.

Hubbard, Barbara. "Taking CDPD's Measure: A Primer." LAN Times. McGraw Hill Companies, October 2, 1995.

Karry, Blake. "Goin' Mobile." Government Technology Press, Government Technology. August, 1997. pp. 42-43.

Koudounas, Vasilis and Iqbal, Omar (1997). "Mobile Computing, Past, Present, and Future."
Distributed Software Engineering Web Shots
http://www-se.doc.ic.ac.uk/~nd/surprise_96/journal/vol4/vk5/report.html#step2

Paone, Joe. "Mobile Data Stalled." LAN Times, The McGraw Hill Companies. February, 1998. P.32

Robert, Jack . "Wireless Field Automation Delivers Results." Radio Resource, Pandanta Corp. March 1998. pp. 52-56.

Rysavy, Peter (1998). "Wide-Area Wireless Computing."
Network Computing Online

http://pubsys.cmp.com/nc/netdesign/wireless6.html

Straight, James (1998). Bell Atlantic. Telephone conversation with authors. McLean, VA, April 1998.

"Survey Highlights: Public Safety Needs." Radio Resource, Pandanta Corp. August 1997. pg. 35.

Tabibian, Ryan O. (1997). "Wireless Data Shootout."
Mobile Computing & Communications Magazine (3)
http://www.mobilecomputing.com/articles/1997/03/9703cr2a.htm

Vahid Koussari (1995). "Wireless Networking With Cellular Digital Packet Data."
City College of New York Web Site
http://www.sci.ccny.cuny.edu/~koussari/wireless/wireless.html

Wireless Data Forum (1997). "CDPD Report Card: CDPD Coverage and Service Available in the U.S. Third Quarter 1997."
Wireless Data Forum Web Site
http://www2.wirelessdata.org/public/newsroom/report_card/newmap.html

Wireless Data Forum (1997). "CDPD Report Card CDPD: Coverage and Service Available in the Northeast U.S. Third Quarter 1997."
Wireless Data Forum Web Site
http://www2.wirelessdata.org/public/newsroom/report_card/newmap.html

Public Safety Wireless Network

PSWN

Digital Land Mobile Radio (DLMR) Security Problem Statement

Final

June 1998

FOREWORD

This problem statement narrative, presented by the Public Safety Wireless Network (PSWN) program, highlights emerging security issues associated with evolving Public Safety radio communications systems. This narrative addresses the vital need for security from an infrastructure protection perspective, explains the cause of new security threats and vulnerabilities, and highlights the security challenges that face the public safety community.

Comments regarding the information contained in this document or for more information regarding the purpose and goals of the PSWN please contact the PSWN Program Management Office (PMO) at 800-565-PSWN or see the web page at www.pswn.gov.

Abstract:

National Performance Review (NPR) recommendation IT04, the Public Safety Wireless Network (PSWN) Management Plan, Executive Order 13010, NPR Action Item A06, and the final report from the President's Commission on Critical Infrastructure Protection (PCCIP) have brought to the forefront of national efforts the protection of the evolving public safety communications infrastructure. Evolving public safety digital land mobile radio (DLMR) systems are envisioned as operating as large automated information systems (AIS) with open interfaces providing digital-based interconnectivity with other systems and subsystems. While the latest DLMR technology will increase the efficiency and effectiveness of public safety communications, a host of security risks could be introduced unless effective mitigating actions are undertaken based on security awareness and understanding. Most importantly, digital radio systems must be configured and managed in a way that will provide adequate protection from computer-based threats. Because the majority of DLMR systems now being rolled out across the country are not undergoing any form of security assurance process, the Public Safety Wireless Network (PSWN) program faces the challenge of investigating and addressing the security issues of the public safety communications infrastructure.

The security-related issues facing the PSWN program are the lack of—

- *An understanding of the security threats, vulnerabilities, and risks associated with the evolving DLMR systems;*
- *Clearly specified communications security needs for public safety organizations;*
- *Security standards or guidelines applicable to DLMR systems; and*
- *An understanding of the tools and techniques available to secure these systems.*

This problem statement reflects concerns first raised in the National Performance Review (NPR) Information Technology initiative 04 (IT04) and the Public Safety Wireless Network (PSWN) Management Plan. These concerns have also been reiterated in Executive Order 13010, NPR's "Access America" Action Item A06, and the final report of the President's Commission on Critical Infrastructure Protection (PCCIP), called Critical Foundations, submitted in October 1997. Executive Order 13010, signed on July 15, 1996, calls for the government and private sector to work together to develop a strategy to protect national critical infrastructures from physical, electronic, radio-frequency, and computer-based attacks and to ensure their continued operation. Emergency services, including medical, police, fire, and rescue, were identified as one of the eight critical infrastructures. In addition, A06, which calls for the establishment of an intergovernmental public safety wireless network, includes the requirement to secure all public safety land mobile radio systems. Clearly, the security of public safety communication infrastructures has been identified as an immediate and critical need. The PCCIP report reiterates the need to protect our nation's information and telecommunications infrastructure, including public safety networks.

As with other critical infrastructures, public safety communication systems depend on the latest technologies for optimum operation. Digital land mobile radio (DLMR) systems represent the future of communications for federal, state, and local public safety agencies throughout the United States. This evolution from analog to digital technology and the development of technical standards will result in greater interconnectivity between public safety system components and a broader range of data transferred on public safety networks. An eventual goal, supported by A06 and its predecessor, IT04, is for greater interoperability across what had been communication boundaries between public safety agencies both vertically (between federal, state, and local) and horizontally (within federal, state, or local). This combination of interconnectivity and interoperability among DLMRs will result in large automated information systems (AIS). It is, in large part, the dependence on automated technologies that makes these systems vulnerable to a host of new threats.

Just as the hacker threat poses a serious security risk to improperly protected AISs, that same threat will now apply to the largely computer-controlled digital radio systems. Depending on the specific system's features, DLMR systems may allow computer-based remote reprogramming, rekeying, talkgroup assignment, and the designation of channels for use by specific talkgroups. Careful assignment of privileges to perform these functions is critical for security. Also, if both local and remote access to the consoles that provide these capabilities is not properly controlled, accidental or malicious reconfiguration or disabling of the radio system could occur. Digital radio systems must be configured and managed in a way that will provide adequate protection from computer-based threats.

The increased use of automated technologies is also driving an increase in the transmission of data in public safety communications. For example, the technology now exists for mobile data terminals (MDTs) running specialized applications to query multiple remote databases for a wide variety of information in a short period of time. However, the DLMR architectures that make this type of data transfer possible may also make it more vulnerable. Public safety sensitive but unclassified (SBU) data will then flow on largely unencrypted networks and reside on computers that may be insufficiently protected. Unchecked, the possible entry points into such a network could expand greatly. For example, a single dial-in modem on any computer on a network could expose the network and its data to unauthorized access. As public safety communication systems become more and more interconnected, security vulnerabilities could continue to expand. Just as with voice communications, security services are needed to ensure the integrity, confidentiality, and availability of the system and the data that it transports and stores. Therefore, while the latest DLMR technology will increase the efficiency and effectiveness of public safety communications, a host of security risks could be introduced unless effective mitigating actions are undertaken.

AISs supporting federal operations, including those of the Department of Defense (DoD), are typically subjected to a security-based certification or assurance process during their development life-cycle in accordance with OMB Circular A-130. OMB A-130 states that information should be protected commensurate with the risk and magnitude of the harm that would result from the loss, misuse, or unauthorized access to or modification of such information. State and local governments, conversely, typically lack their own security standards and may look to federal security standards or industry best security practices for guidance in planning, developing, and operating their AISs.

The assurance process is designed to ensure that the necessary technical and procedural security controls are incorporated into the system and its operation to ensure a low level of risk for the overall security of the system. The process may vary between systems, but it typically includes, at a minimum, the development of a security policy, the identification of security requirements, and the performance of a security review (risk assessment) and/or security test and evaluation of the system against its requirements to verify compliance. These requirements may cover a broad range of security domains including computer, personnel, physical, and administrative security. Any failure to meet a requirement may represent a security vulnerability. There is a security risk internal or external to the site if threats exist that could exploit the vulnerability. The majority of DLMR systems now being rolled out across the country are not undergoing any form of security assurance process.

LMR system users and managers may be well aware of traditional LMR security risks and means of protection. Traditional security controls are relatively straightforward and involve the use of some form of encryption for radio frequency (RF) communications, physical protection of equipment, and layers of redundancy in the system for contingency purposes. These individuals, however, are typically unfamiliar with the security threats, vulnerabilities, and resulting risks associated with newer DLMR

technologies and system architectures. They may also be unfamiliar with the proper use or configuration of security controls offered with the newer DLMR product lines. The DLMR products may lack appropriate security controls or offer them as optional features. This lack of awareness or understanding of the more AIS-like risks and available security controls associated with modern DLMR systems increases the likelihood that security breaches will occur. Examples of AIS-like technical security controls that may be unfamiliar to traditional LMR users and managers include password protection, file access control, security audit log capture and review, and packet filtering routers or application firewalls to protect interconnected networks. Without appropriate controls, it is more likely that security breaches will go undetected.

The PSWN program, in its overall effort to support the evolution of public safety DLMR systems towards nationwide interoperability, has the challenge of investigating and addressing security issues.

The security-related issues facing the PSWN program are the lack of —

- An understanding of the security threats, vulnerabilities, and risks associated with the evolving DLMR systems;
- Clearly specified communications security needs for public safety organizations;
- Security standards or guidelines applicable to DLMR systems; and
- An understanding of the tools and techniques available to secure these systems.